PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-272561
(43)Date of publication of application : 08.10.1999

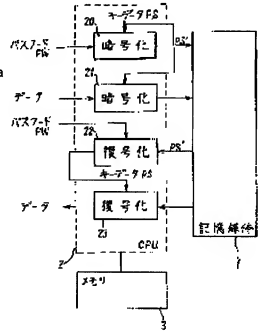
(51)Int.Cl. G06F 12/14
G06F 3/06

(21)Application number : 10-068881
(22)Date of filing : 18.03.1998

(71)Applicant : FUJITSU LTD
(72)Inventor : KOBAYASHI HIROYUKI
UCHIDA YOSHIAKI

(54) DATA PROTECTION METHOD FOR STORAGE MEDIUM DEVICE FOR THE SAME AND STORAGE MEDIUM THEREFOR

(57)Abstract:
PROBLEM TO BE SOLVED: To change key data for each storage unit by one word in a data protection method for a storage medium and its device which encipher data to be recorded in the storage medium by a password and perform protection of the data.
SOLUTION: This device has a step which has a password PW encipher 20 key data P5 and writes them in a storage medium 1 after generating the key data P5 and a step which has the key data encipher 21 data and write them in the storage medium 1. Moreover, it has a step which reads the enciphered key data from the storage medium 1, a step which has the password decode 22 the enciphered key data, and a step which has the decoded key data decode 23 the data of the storage medium 1. Since enciphering is performed by using the key data generated separately from the password, an analysis of the password by decoding of a cryptogram is prevented.



LEGAL STATUS

[Date of request for examination] 01.02.2005

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

(19)日本国特許庁（ＪＰ）　(12) 公開特許公報（A）　(11)特許出願公開番号

特開平11－272561

(43)公開日　平成11年(1999)10月８日

(51)Int.Cl.⁶	識別記号	ＦＩ	
Ｇ０６Ｆ　12/14	３２０	Ｇ０６Ｆ　12/14	３２０Ｂ
3/06	３０４	3/06	３０４Ｈ

審査請求　未請求　請求項の数15　ＯＬ　（全 18 頁）

(21)出願番号　特願平10－68881

(22)出願日　平成10年(1998) ３月18日

(71)出願人　000005223
富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番１号

(72)発明者　小林　弘幸
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

(72)発明者　内田　好昭
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

(74)代理人　弁理士　林　恒徳　（外１名）

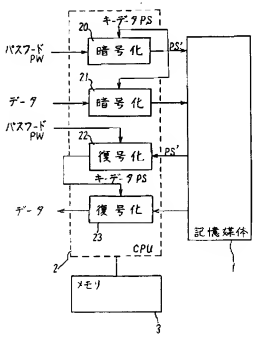
(54)【発明の名称】　記憶媒体のデータ保護方法、その装置及びその記憶媒体

(57)【要約】

【課題】　記憶媒体に記録するデータをパスワードにより暗号化して、データの保護を行うための記憶媒体のデータ保護方法及びその装置に関し、一つのパスワードで、各記憶単位に、キーデータを変える。

【解決手段】　キーデータを生成した後、キーデータをパスワードによって暗号化して、記憶媒体１に書き込むステップと、キーデータによりデータを暗号化して、記憶媒体１に書き込むステップとを有する。更に、記憶媒体１から暗号化されたキーデータを読みだすステップと、暗号化されたキーデータをパスワードで復号化するステップと、復号化されたキーデータで記憶媒体１のデータを復号化するステップとを有する。パスワードと別に生成するキーデータを用いて暗号化するので、暗号文の解読によるパスワードの解析を防止することができる。

ブロック図



【特許請求の範囲】

【請求項１】　記憶媒体のデータを保護するための記憶媒体のデータ保護方法において、
キーデータを生成して、前記キーデータをパスワードによって暗号化して、前記記憶媒体に書き込むステップと、
前記キーデータによりデータを暗号化して、前記記憶媒体に書き込むステップと、
前記記憶媒体から前記暗号化されたキーデータを読みだすステップと、
前記暗号化されたキーデータを前記パスワードで復号化するステップと、
前記復号化されたキーデータで前記記憶媒体のデータを復号化するステップとを有することを特徴とする記憶媒体のデータ保護方法

【請求項２】　請求項１の記憶媒体のデータ保護方法において、
前記キーデータを生成するステップは、
前記記憶媒体の論理セクタ毎に、前記キーデータを生成するステップであることを特徴とする記憶媒体のデータ保護方法.

【請求項３】　請求項２の記憶媒体のデータ保護方法において、
前記キーデータを生成するステップは、
前記データの書き込み時に、前記論理セクタ毎に前記キーデータを生成するステップであることを特徴とする記憶媒体のデータ保護方法.

【請求項４】　請求項１の記憶媒体のデータ保護方法において、
前記キーデータを生成するステップは、予め定められた数のランダムデータを組み合わせて、前記キーデータを生成するステップであることを特徴とする記憶媒体のデータ保護方法.

【請求項５】　請求項１の記憶媒体のデータ保護方法において、
前記記憶媒体から前記暗号化されたキーデータを読み出した後、使用者が指定した旧パスワードにより復号化するステップと、
前記復号化されたキーデータを、使用者が指定した新パスワードにより暗号化した後、前記記憶媒体に暗号化したキーデータを書き込むステップとを有することを特徴とする記憶媒体のデータ保護方法

【請求項６】　請求項１の記憶媒体のデータ保護方法において、
前記暗号化されたキーデータを前記記憶媒体に書き込むステップは、
複数のパスワードの各々で、前記キーデータを暗号化して、前記各暗号化されたキーデータを前記記憶媒体に書き込むステップであり、
前記キーデータを復号化するステップは、
前記読みだした暗号化されたキーデータを指定されたパスワードで復号化するステップであることを特徴とする記憶媒体のデータ保護方法.

【請求項７】　請求項１の記憶媒体のデータ保護方法において、
前記暗号化されたキーデータを前記記憶媒体に書き込むステップは、
一のパスワードで、前記キーデータを暗号化して、前記暗号化されたキーデータを前記記憶媒体に書き込み且つ一のパスワードで他のパスワードを暗号化して、暗号化された他のパスワードを書き込むステップであり、
前記キーデータを復号化するステップは、
前記暗号化された他のパスワードを前記他のパスワードで復号化して、前記一のパスワードを得るステップと、
前記暗号化されたキーデータを前記一のパスワードで復号化するステップであることを特徴とする記憶媒体のデータ保護方法

【請求項８】　記憶媒体のデータを保護するための記憶媒体のデータ保護装置において、
記憶媒体と、
前記記憶媒体のデータをリード及びライトする制御回路とを有し、
前記制御回路は、
キーデータを生成した後、前記キーデータをパスワードによって暗号化して、前記記憶媒体に書き込み且つ前記キーデータによりデータを暗号化して、前記記憶媒体に書き込むライトモードと、
前記記憶媒体から前記暗号化されたキーデータを読みだした後、前記暗号化されたキーデータを前記パスワードで復号化し、且つ前記復号化されたキーデータで前記記憶媒体のデータを復号化するリードモードとを有することを特徴とする記憶媒体のデータ保護装置.

【請求項９】　請求項８の記憶媒体のデータ保護装置において、
前記記憶媒体は、論理セクタ毎にリード／ライトされる記憶媒体で構成され、
前記制御回路は、前記記憶媒体の論理セクタ毎に、前記キーデータを生成することを特徴とする記憶媒体のデータ保護装置.

【請求項１０】　請求項９の記憶媒体のデータ保護装置において、
前記制御回路は、前記データの書き込み時に、前記論理セクタ毎に前記キーデータを生成することを特徴とする記憶媒体のデータ保護装置

【請求項１１】　請求項８の記憶媒体のデータ保護装置において、
前記制御回路は、予め定められた数のランダムデータを組み合わせて、前記キーデータを生成することを特徴とする記憶媒体のデータ保護装置.

【請求項１２】　請求項８の記憶媒体のデータ保護装置

において、
前記制御回路は、
前記記憶媒体から前記暗号化されたキーデータを読み出した後、使用者が指定した旧パスワードにより復号化し、且つ前記復号化されたキーデータを、使用者が指定した新パスワードにより暗号化した後、前記記憶媒体に暗号化したキーデータを書き込むことを特徴とする記憶媒体のデータ保護装置。
【請求項１３】　請求項８の記憶媒体のデータ保護装置において、
前記制御回路は、
複数のパスワードの各々で、前記キーデータを暗号化して、前記各暗号化されたキーデータを前記記憶媒体に書き込むライトモードと、
前記読みだした暗号化されたキーデータを指定されたパスワードで復号化するリードモードとを有することを特徴とする記憶媒体のデータ保護装置。
【請求項１４】　請求項８の記憶媒体のデータ保護装置において、
前記制御回路は、
一のパスワードで、前記キーデータを暗号化して、前記暗号化されたキーデータを前記記憶媒体に書き込み且つ一のパスワードで他のパスワードを暗号化して、暗号化された他のパスワードを書き込むライトモードと、
前記暗号化された他のパスワードを前記他のパスワードで復号化して、前記一のパスワードを得た後、前記暗号化されたキーデータを前記一のパスワードで復号化するリードモードとを有することを特徴とする記憶媒体のデータ保護装置。
【請求項１５】　保護されたデータを有する記憶媒体において、
パスワードによって暗号化されたキーデータと、
前記キーデータによって暗号化されたデータとを有することを特徴とする記憶媒体。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、情報処理機器において、記憶媒体に記録するデータをパスワードにより暗号化して、データの保護を行うための記憶媒体のデータ保護方法、その装置及びその記憶媒体に関する
【０００２】光ディスク、磁気ディスク、ＩＣカード等を利用した記憶装置は、コンピュータ、ワードプロセッサ、電子ブック等の様々な情報処理機器に利用されている。この記憶装置では、プライバシィに係わる情報や職務上の機密情報など、本来所有者以外に知られたくない情報が書き込まれることがある。このような情報を他人に知られないようにするため、データを暗号化することが必要となる
【０００３】
【従来の技術】図１５は、従来技術の説明図である。
【０００４】光ディスク等の記憶媒体９０又は記憶装置に対し、パスワードを設定する。データの書き込みに際しては、暗号化部９１によりデータをパスワードで暗号化して、記憶媒体９０に書き込む。又、読み出し時には、復号化部９２により記憶媒体９０のデータをパスワードで復号化する。
【０００５】このように、データを暗号化することにより、データの秘匿を行うことができる。この場合に、従来、記憶媒体全体に１つのパスワードを設定する方式があった。又、記憶媒体のファイル単位に異なるパスワードを設定する方式もある。
【０００６】
【発明が解決しようとする課題】しかしながら、従来技術では、次の問題があった。
【０００７】第１に、サンプルとしての暗号文又は暗号文と暗号化されていない平文の組み合わせが多い程、解読者の解読が容易となる。同一の平文を同一のパスワードで暗号化した結果は、等しいので、同一のパスワードで直接暗号化した場合には、暗号文の統計的性質は、平文の統計的性質を反映する。従って、従来の記憶媒体を同一のパスワードで暗号化する方式では、暗号文が統計処理できる程多量にあれば、平文の性質を容易に推定できるという問題があった。
【０００８】第２に、光ディスク等の大容量記憶媒体に保存されているデータには、そのディレクトリ部分などの定型フォーマットで構成されている部分がある。従来の記憶媒体を同一のパスワードで暗号化する方式では、このような部分を解析することにより、パスワードを推定すると、他の重要なデータも解読されてしまうという問題があった。
【０００９】第３に、従来のファイル毎に、パスワードを設定する方式では、一部分のパスワードの解読により、他の部分の解読を防止できる。しかし、この場合、ファイル毎に、異なるパスワードを管理する必要がある。このため、煩雑であり、パスワード忘却等の事故を招きやすいという問題があった。
【００１０】第４に、光ディスク等の交換可能な大容量記憶媒体においては、記憶媒体を持ち出したり、記憶媒体を複写することが可能である。このため、一旦暗号化されたデータを持ち出し、ゆっくりと解析することが可能である。従って、暗号文からパスワードを推定しやすいという問題もあった。
【００１１】第５に、従来は、パスワードで直接暗号化していたため、パスワードを変えると、データ全体を再暗号化する必要があるという問題もあった。
【００１２】本発明の目的は、暗号文からパスワードが解析されにくい記憶媒体のデータ保護方法、その装置及びその記憶媒体を提供することにある
【００１３】本発明の他の目的は、一つのパスワードで、各記憶単位に、キーデータを変えることができる記

憶媒体のデータ保護方法、その装置及びその記憶媒体を提供することにある。

【００１４】本発明の更に他の目的は、パスワードを変えても、データの再暗号化を不要とする記憶媒体のデータ保護方法、その装置及びその記憶媒体を提供することにある。

【００１５】

【課題を解決するための手段】本発明の記憶媒体のデータ保護方法は、キーデータを生成した後、前記キーデータをパスワードによって暗号化して、前記記憶媒体に書き込むステップと、キーデータによりデータを暗号化して、前記記憶媒体に書き込むステップとを有する書き込みモードを有する。そして、そのデータ保護方法は、記憶媒体から前記暗号化されたキーデータを読みだすステップと、暗号化されたキーデータを前記パスワードで復号化するステップと、復号化されたキーデータで前記記憶媒体のデータを復号化するステップとを有するリードモードとを有する。

【００１６】本発明では、パスワードをそのまま暗号化キーとして用いるのではなく、パスワードとは、別に生成したキーデータを用いて、データを暗号化する　キーデータは、パスワードをキーとして暗号化して、記憶媒体に書き込む。読み出し時には、パスワードにより、暗号化されたキーデータを復号化して、キーデータを得る。そして、キーデータでデータを復号化する

【００１７】このようにパスワードとは、別に生成したキーデータを用いて、データを暗号化することにより、暗号文を解析しても、暗号化されたキーデータが解読されるだけである。このため、パスワードやキーデータを解析しにくい。これにより、暗号文の解析によるパスワードの解読を防止できる

【００１８】又、パスワードとは、別に生成したキーデータを用いて、暗号化するため、１つのパスワードに対し、キーデータを変えることにより、セクタ等の記憶単位に異なるキーを付与できる。このため、論理セクタ毎に異なるキーを用いて、暗号化でき、データの機密性を高めることができる。

【００１９】更に、パスワードとは、別に生成したキーデータを用いて、暗号化するため、パスワードを変えても、データの再暗号化が不要となる　このため、数百メガバイトの大容量記憶媒体でも、容易にパスワードの変更を実現できる。

【００２０】

【発明の実施の形態】図１は、本発明の一実施の形態のブロック図、図２は、本発明の第１の実施の形態の論理フォーマット時の処理フロー図、図３は、本発明の第１の実施の形態の書き込み処理フロー図、図４は、本発明の第１の実施の形態の記憶領域の説明図、図５は、本発明の第１の実施の形態のキーデータの説明図、図６は、本発明の第１の実施の形態の読み出し処理フロー図である。

【００２１】図１に示すように、記憶媒体１は、光磁気ディスクで構成されている。この記憶媒体１の論理セクタサイズを、２ＫＢ（キロバイト）とする。制御回路２は、プロセッサで構成されている　第１の暗号化部２０は、キーデータＰＳを使用者が入力したパスワードＰＷにより暗号化し、且つ暗号化したキーデータＰＳ’を記憶媒体１に書き込む。

【００２２】第２の暗号化部２１は、書き込むべきデータをキーデータＰＳで暗号化し、暗号化されたデータを記憶媒体１に書き込む。第１の復号化部２２は、記憶媒体１の暗号化されたキーデータＰＳ’を、使用者が入力したパスワードＰＷで復号化する。第２の復号化部２３は、復号化されたキーデータＰＳにより、記憶媒体１のデータを復号化して、データを出力する。メモリ３は、制御回路（以下、ＣＰＵという）２の作業域を与えるものである。尚、第１、第２の暗号化部２０、２１、第１、第２の復号化部２２、２３は、ＣＰＵ２の処理をブロックにして示したものである。

【００２３】図２により、媒体の論理フォーマット作成時の処理について、説明する。媒体の初期処理である媒体の論理フォーマット作成時に、以下の処理を実行する。

【００２４】（Ｓ１）使用者は、ユーザーパスワードＰＷをＣＰＵ２に入力する。

【００２５】（Ｓ２）ＣＰＵ２は、セクタ数分の乱数（８バイト）を発生する　この乱数が、キーデータＰＳである。以下、セクタ数をｎとし、ＰＳ〔１〕～ＰＳ〔ｎ〕の乱数を生成したものとして説明する。

【００２６】（Ｓ３）ＣＰＵ２は、このセクタ数分の乱数（ランダムデータ）ＰＳ〔　〕（ＰＳ〔１〕～ＰＳ〔ｎ〕）を、メモリ３の作業域に格納する。

【００２７】（Ｓ４）ＣＰＵ２は、作業域のキーデータＰＳ〔１〕～ＰＳ〔ｎ〕の各々を、パスワードＰＷで暗号化する　もちろん、作業域のキーデータＰＳ〔１〕～ＰＳ〔ｎ〕の全体をパスワードＰＷで暗号化しても構わない

【００２８】（Ｓ５）ＣＰＵ２は、暗号化されたキーデータＰＳ’〔１〕～ＰＳ’〔ｎ〕を記憶媒体１の領域Ｌ１に書き込む。

【００２９】図４に示すように、記憶媒体（ディスク）１の論理フォーマットは、各セクタで示される　このセクタは、論理ブロックアドレスＬＢＡによりアドレスされる　ここで、図では、ＬＢＡが、「１」から「Ｘ」までＸ個のセクタが設けられている

【００３０】この光ディスクの記憶領域の内、先頭セクタ（ＬＢＡ＝１）からａセクタ分の領域Ｌ１を、暗号化されたキーデータＰＳ’〔１〕～ＰＳ’〔ｎ〕の格納領域に割り当てる　即ち、データの使用域のセクタ数は、ｎ（＝（Ｘ－ａ））であり、各使用域のセクタ毎に、第

域Ｌ１に、暗号化されたキーデータＰＳ’〔１〕～ＰＳ’〔ｎ〕が格納される。

【００３１】次に、媒体の書き込み処理について、図３により説明する。

【００３２】（Ｓ１０）論理ブロックアドレス（セクタ番号）ＬＢＡが、「Ｓ０」の位置への書き込み要求が生じたとする。書き込み要求する位置が、領域Ｌ１と重ならないようにするため、要求されたセクタ番号ＬＢＡを、「Ｓ１」に変更する。ここでは、図４に示したように、セクタ番号「Ｓ０」に、領域Ｌ１の大きさ「ａ」を加えて、変更されたセクタ番号「Ｓ１」を得る。

【００３３】（Ｓ１１）ＣＰＵ２は、光ディスク１の領域Ｌ１のデータ（暗号化されたキーデータ）を読み出し済かを判定する。読み出し済ならば、メモリ３の作業域に、キーデータが展開されているため、ステップＳ１４に進む。

【００３４】（Ｓ１２）ＣＰＵ２は、領域Ｌ１のデータが読み出し済でないなら、メモリ３の作業域に、キーデータを展開する処理を行う。即ち、ＣＰＵ２は、ユーザーハスワードＰＷを得る。そして、光ディスク１の領域Ｌ１のデータＰＳ’〔１〕～ＰＳ’〔ｎ〕を読みだす。

【００３５】（Ｓ１３）ＣＰＵ２は、領域Ｌ１のデータＰＳ’〔１〕～ＰＳ’〔ｎ〕を、ハスワードＰＷで復号化する。これにより、キーデータＰＳ〔１〕～ＰＳ〔ｎ〕が得られる。このキーデータＰＳ〔　〕（ＰＳ〔１〕～ＰＳ〔ｎ〕）を、メモリ３の作業域に格納する。

【００３６】（Ｓ１４）ＣＰＵ２は、メモリ３の作業域のキーデータから、論理ブロックアドレス（セクタ番号）ＬＢＡ（＝Ｓ０）のキーデータＰＳ〔Ｓ０〕を得る。図５に示すように、メモリ３の作業域のキーデータテーブルから論理ブロックアドレスＬＢＡに対応するキーデータＰＳ〔Ｓ０〕が得られる。そして、ＣＰＵ２は、書き込むべきデータを、このキーデータＰＳ〔Ｓ０〕で暗号化する。暗号化の方法としては、周知のＤＥＳ等を用いることができる。

【００３７】（Ｓ１５）ＣＰＵ２は、この暗号化されたデータを、光ディスク１の論理ブロックアドレスＬＢＡ（＝Ｓ１）の位置に書き込む。

【００３８】次に、図６を用いて、読み出し処理を説明する。

【００３９】（Ｓ２０）論理ブロックアドレス（セクタ番号）ＬＢＡが「Ｓ０」の位置への読み出し要求が生じたとする。読み出し要求する位置が、領域Ｌ１と重ならないようにするため、要求されたセクタ番号ＬＢＡを、「Ｓ１」に変更する。ここでは、図４に示したように、セクタ番号「Ｓ０」に、領域Ｌ１の大きさ「ａ」を加えて、変更されたセクタ番号「Ｓ１」を得る。

【００４０】（Ｓ２１）ＣＰＵ２は、光ディスク１の領域Ｌ１のデータ（暗号化されたキーデータ）を読み出し済かを判定する。読み出し済ならば、メモリ３の作業域に、キーデータが展開されているため、ステップＳ２４に進む。

【００４１】（Ｓ２２）ＣＰＵ２は、領域Ｌ１のデータが読み出し済でないなら、メモリ３の作業域に、キーデータを展開する処理を行う。即ち、ＣＰＵ２は、ユーザーハスワードＰＷを得る。そして、光ディスク１の領域Ｌ１のデータＰＳ’〔１〕～ＰＳ’〔ｎ〕を読みだす。

【００４２】（Ｓ２３）ＣＰＵ２は、領域Ｌ１のデータＰＳ’〔１〕～ＰＳ’〔ｎ〕を、ハスワードＰＷで復号化する。これにより、キーデータＰＳ〔１〕～ＰＳ〔ｎ〕が得られる。このキーデータＰＳ〔　〕（ＰＳ〔１〕～ＰＳ〔ｎ〕）を、メモリ３の作業域に格納する。

【００４３】（Ｓ２４）ＣＰＵ２は、メモリ３の作業域のキーデータから、論理ブロックアドレス（セクタ番号）ＬＢＡ（＝Ｓ０）のキーデータＰＳ〔Ｓ０〕を得る。図５に示すように、メモリ３の作業域のキーデータテーブルから論理ブロックアドレスＬＢＡに対応するキーデータＰＳ〔Ｓ０〕が得られる。そして、ＣＰＵ２は、論理ブロックアドレスＳ１のデータを、光ディスク１から読みだす。更に、ＣＰＵ２は、読みだしたデータをキーデータＰＳ〔Ｓ０〕で復号化する。復号化の方法としては、周知のＤＥＳ等を用いることができる。復号化されたデータを要求元（例えば、コンピュータ）に送りだす。

【００４４】このようにして、媒体の論理フォーマット作成時に、論理セクタ毎に、乱数を発生して、論理セクタ毎のキーデータを生成する。そして、記憶媒体１に、ハスワードで暗号化されたキーデータを書き込んでおく。データの書き込み時には、キーデータによりデータを暗号化して、記憶媒体１に書き込む。

【００４５】データの読み取り時には、記憶媒体１の暗号化されたキーデータを読み出した後、ハスワードで復号化して、キーデータを得る。そして、記憶媒体から読みだしたデータを、このキーデータにより復号化する。

【００４６】このように、ハスワードとは別に生成したキーデータにより、データを暗号化することにより、暗号文を解析しても、暗号化されたキーデータが解読されるだけである。このため、ハスワードやキーデータを解析しにくい。これにより、暗号文の解析によるハスワードの解読を防止できる。

【００４７】又、ハスワードとは、別に生成したキーデータを用いて、暗号化するため、１つのハスワードに対し、キーデータを変えることにより、論理セクタ単位に異なるキーを付与できる。このため、論理セクタ毎に異なるキーを用いて、暗号化でき、データの機密性を高めることができる。

【００４８】尚、領域Ｌ１を論理ブロックアドレスの小さい方に設けているが、領域Ｌ１を論理ブロックアドレ

スの最大の部分に格納しても良い。

【0049】図7は、本発明の第2の実施の形態の書き込み処理フロー図である。図7により、媒体の書き込み処理について、説明する。媒体の論理フォーマット作成時の処理は、図2の実施の形態と同様に行い、記憶媒体1に各論理セクタの暗号化されたキーデータを格納しておく。

【0050】（S30）論理ブロックアドレス（セクタ番号）LBAが「S0」の位置への書き込み要求が生じたとする。書き込み要求する位置が、領域L1と重ならないようにするため、要求されたセクタ番号LBAを、「S1」に変更する。ここでは、図4に示したように、セクタ番号「S0」に、領域L1の大きさ「a」を加えて、変更されたセクタ番号「S1」を得る。

【0051】（S31）CPU2は、光ディスク1の領域L1のデータ（暗号化されたキーデータ）を読み出し済かを判定する。読み出し済なら、メモリ3の作業域に、キーデータが展開されているため、ステップS34に進む。

【0052】（S32）CPU2は、領域L1のデータが読み出し済でないなら、メモリ3の作業域に、キーデータを展開する処理を行う。即ち、CPU2は、ユーザーパスワードPWを得る。そして、光ディスク1の領域L1のデータPS’〔1〕～PS’〔n〕を読みだす。

【0053】（S33）CPU2は、領域L1のデータPS’〔1〕～PS’〔n〕を、パスワードPWで復号化する。これにより、キーデータPS〔1〕～PS〔n〕が得られる。このキーデータPS〔　〕（PS〔1〕～PS〔n〕）を、メモリ3の作業域に格納する。

【0054】（S34）CPU2は、乱数Rを発生する。そして、CPU2は、メモリ3の作業域のキーデータの論理ブロックアドレス（セクタ番号）LBA（＝S0）のキーデータPS〔S0〕に、乱数Rを書き込む。

【0055】（S35）そして、CPU2は、書き込むべきデータを、このキーデータPS〔S0〕（乱数R）で暗号化する。暗号化の方法としては、周知のDES等を用いることができる。CPU2は、この暗号化されたデータを、光ディスク1の論理ブロックアドレスLBA（＝S1）の位置に書き込む。

【0056】（S36）CPU2は、適当なタイミングで、光ディスク1の領域L1のデータを書き換える。即ち、CPU2は、書き込み回数を示す書き込みカウンタの値WCが、例えば、32回を越えた場合には、安全のため、領域L1を書き換えるため、ステップS37に進む。一定回数毎に書き込むのは、何らかの異常により媒体排出等の処理がなされない事態が生じても、ある程度のデータ回復を保証するためのものである。32回という数値に任意である。この処理は本発明の必須要件ではない。又、CPU2は、記憶媒体1の排出要求があった場合に、キーデータを保存するため、ステップS37に進む。更に、CPU2は、電源のオフが生じた場合に、キーデータを保存するため、ステップS37に進む。

【0057】（S37）CPU2は、作業域のキーデータPS〔1〕～PS〔n〕の各々を、パスワードPWで暗号化する。もちろん、作業域のキーデータPS〔1〕～PS〔n〕の全体をパスワードPWで暗号化しても構わない。次に、CPU2は、暗号化されたキーデータPS’〔1〕～PS’〔n〕を記憶媒体1の領域L1に書き込む。

【0058】この第2の実施の態様では、第1の実施の形態の作用に加えて、データの書き込み毎に、異なるキーデータを生成する。このため、データの書き込み毎に、異なるキーデータで暗号化され、データの秘匿性が向上する。

【0059】尚、読み出し処理は、図6の第1の実施の形態と同一であるので、説明を省略する。

【0060】図8は、本発明の第3の実施の形態の書き込み処理フロー図、図9は、本発明の第3の実施の形態のキーデータの説明図、図10は、本発明の第3の実施の形態の読み出し処理フロー図である。

【0061】媒体の論理フォーマット時には、図2で示した第1の実施の形態と同様にして、光ディスク1の領域L1に、暗号化されたキーデータPS’〔1〕～PS’〔512〕を格納する。但し、ここでは、各論理セクタ毎に、暗号化されたキーデータを格納しない。例えば、領域L1の大きさを4KBとする。そして、ハスワードを8バイト／エントリとすると、図9に示すように、512個（エントリ）のキーワードPS〔1〕～PS〔512〕を生成する。そして、領域L1には、512個の暗号化されたキーワードPS’〔1〕～PS’〔512〕を格納する。

【0062】図8により、書き込み処理について、説明する。

【0063】（S40）論理ブロックアドレス（セクタ番号）LBA「S0」の位置への書き込み要求が生じたとする。書き込み要求する位置が、領域L1と重ならないようにするため、要求されたセクタ番号LBAを、「S1」に変更する。ここでは、図4に示したように、セクタ番号「S0」に、領域L1の大きさ「a」を加えて、変更されたセクタ番号「S1」を得る。

【0064】（S41）CPU2は、光ディスク1の領域L1のデータ（暗号化されたキーデータ）を読み出し済かを判定する。読み出し済なら、メモリ3の作業域に、キーデータが展開されているため、ステップS44に進む。

【0065】（S42）CPU2は、領域L1のデータが読み出し済でないなら、メモリ3の作業域に、キーデータを展開する処理を行う。即ち、CPU2は、ユーザーパスワードPWを得る。そして、光ディスク1の領域

L1のデータPS'〔1〕～PS'〔n〕を読みだす。

【0066】（S43）CPU2は、領域L1のデータPS'〔1〕～PS'〔n〕を、パスワードPWで復号化する。これにより、キーデータPS〔1〕～PS〔n〕が得られる。このキーデータPS〔 〕（PS〔1〕～PS〔n〕）を、メモリ3の作業域に格納する。

【0067】（S44）CPU2は、要求されたセクタ番号S0から4つの値R0、R1、R2、R3を得る。ここでは、論理セクタ番号S0を32ビットのビット列と見なし、8ビットづつを1つの値R0、R1、R2、R3に纏める。R0～R3は、0以上256未満の値になる。そして、R0～R3をインデックスとして、メモリ3の作業域のPS〔 〕から乱数値（キーデータ）を取り出す。取り出した4つの値を基に、8バイトの乱数（キーデータ）Rを発生する。

【0068】ここでは、図9に示すように、R0に対応するキーデータPS〔R0〕を取り出し、（R1＋256）に対応するキーデータPS〔R1＋256〕を取り出す。R2に対応するキーデータPS〔R2＋256〕を取り出し、R3に対応するキーデータPS〔R3〕を取り出す。

【0069】そして、下記演算式により、キーデータRを演算する。

【0070】

R＝（PS〔R0〕＊PS〔R1＋256〕）
＊（PS〔R2＋256〕＋PS〔R3〕）

尚、「＊」は、EOR演算である。

【0071】（S45）そして、CPU2は、書き込むべきデータを、このキーデータRで暗号化する。暗号化の方法としては、周知のDES等を用いることができる。CPU2は、この暗号化されたデータを、光ディスク1の論理ブロックアドレスLBA（＝S1）の位置に書き込む。

【0072】次に、図10により、読み出し処理を説明する。

【0073】（S50）論理ブロックアドレス（セクタ番号）LBAが「S0」の位置への読み出し要求が生じたとする。読み出し要求する位置が、領域L1と重ならないようにするため、要求されたセクタ番号LBAを、「S1」に変更する。ここでは、図4に示したように、セクタ番号「S0」に、領域L1の大きさ「a」を加えて、変更されたセクタ番号「S1」を得る。

【0074】（S51）CPU2は、光ディスク1の領域L1のデータ（暗号化されたキーデータ）を読み出し済みか判定する。読み出し済みなら、メモリ3の作業域に、キーデータが展開されているため、ステップS54に進む。

【0075】（S52）CPU2は、領域L1のデータが読み出し済みでないなら、メモリ3の作業域に、キーデータを展開する処理を行う。即ち、CPU2は、ユーザーパスワードPWを得る。そして、光ディスク1の領域L1のデータPS'〔1〕～PS'〔n〕を読みだす。

【0076】（S53）CPU2は、領域L1のデータPS'〔1〕～PS'〔n〕を、パスワードPWで復号化する。これにより、キーデータPS〔1〕～PS〔n〕が得られる。このキーデータPS〔 〕（PS〔1〕～PS〔n〕）を、メモリ3の作業域に格納する。

【0077】（S54）CPU2は、要求されたセクタ番号S0から4つの値R0、R1、R2、R3を得る。論理セクタ番号S0を32ビットのビット列と見なし、8ビットづつを1つの値R0、R1、R2、R3に纏める。そして、R0～R3をインデックスとして、メモリ3の作業域のPS〔 〕から乱数値（キーデータ）を取り出す。取り出した4つの値を基に、8バイトの乱数（キーデータ）Rを発生する。

【0078】ここでは、図9に示すように、R0に対応するキーデータPS〔R0〕を取り出し、（R1＋256）に対応するキーデータPS〔R1＋256〕を取り出す。R2に対応するキーデータPS〔R2＋256〕を取り出し、R3に対応するキーデータPS〔R3〕を取り出す。

【0079】そして、上述した演算式より、キーデータRを演算する。

【0080】（S55）そして、CPU2は、光ディスク1から論理ブロックアドレスLBA（＝S1）のデータを読みだす。更に、読みだしたデータを、このキーデータRで復号化する。復号化の方法としては、周知のDES等を用いることができる。

【0081】この第3の実施の形態では、第1の実施の形態に比し、光ディスク1の領域L1の大きさを小さくできる。即ち、第1の実施の形態では、論理セクタの数と同数のキーデータを格納する必要がある。例えば、1セクタを2KBとし、記憶容量を600MBとし、キーデータを8Byteとすると、領域L1は、2.4MBの容量が必要となる。第3の実施の形態では、512個のキーデータを格納するので、領域L1は4KB程度で済む。

【0082】しかも、このようにしても、演算により乱数を発生するので、セクタ毎に異なるキーデータが得られる。

【0083】図11は、本発明の第4の実施の形態の説明図、図12は、本発明の第4の実施の形態の書き込み処理フローである。

【0084】この第4の実施の形態は、第3の実施の形態に加えて、複数のユーザーパスワードを使用できる方法を示すものである。図11に示すように、使用者をn名まで認めるため、各使用者毎に、パスワードPW1～PWnを設定する。パスワードが8バイトであるとし

て、各使用者に対応して、８バイト（ＰＷｉの大きさ）の領域Ｌ２～Ｌｎと、８バイトの領域Ｃ１～Ｃｎを、光ディスク１に設ける

【００８５】記憶媒体の論理フォーマットを作成する時は、第３の実施の形態と同様に、領域Ｌ１に、乱数データをユーザーパスワードＰＷ１により暗号化したものを書き込んでおく

【００８６】それに加えて、パスワードの検証用文字列ＤＣ１を生成し、これをパスワードＰＷ１で暗号化したものを領域Ｃ１に書き込んでおく。更に、パスワードＰＷ１をＰＷ２で暗号化したものを、領域Ｌ２に書き込み、パスワードＰＷ１をＰＷｎで暗号化したものを、領域Ｌｎに書き込む。

【００８７】更に、パスワードＰＷ２の検証用文字列ＤＣ２をパスワードＰＷ２で暗号化したものを、領域Ｃ２に書き込む。以下、パスワードＰＷｎの検証用文字列ＤＣｎをパスワードＰＷｎで暗号化したものを、領域Ｃｎに書き込む。

【００８８】各パスワードの検証用文字列は、入力したパスワードが正しいかを検証するものである。この検証用文字列は、システムに特有の秘密の文字列で構成しても良く、パスワードＰＷｉから計算される値（例えば、パスワードＰＷｉとある特定の文字列との排他的論理和）としても良い。

【００８９】次に、ユーザーパスワードを用いる場合のデータの書き込み、読み出し処理は、図８及び図１０に示した第３の実施の形態と同様に行う。

【００９０】ユーザーパスワードＰＷｉ（ｉ＞１）を用いる場合のデータの書き込みは、図１２により説明する。

【００９１】（Ｓ６０）論理ブロックアドレス（セクタ番号）ＬＢＡが「Ｓ０」の位置への書き込み要求が生じたとする。書き込み要求する位置が、領域Ｌ１と重ならないようにするため、要求されたセクタ番号ＬＢＡを、「Ｓ１」に変更する。ここでは、図４に示したように、セクタ番号「Ｓ０」に、領域Ｌ１の大きさ「ａ」を加えて、変更されたセクタ番号「Ｓ１」を得る。

【００９２】（Ｓ６１）ＣＰＵ２は、光ディスク１の領域Ｌ１のデータ（暗号化されたキーデータ）を読み出し済かを判定する。読み出し済なら、メモリ３の作業域に、キーデータが展開されているため、ステップＳ６４に進む。

【００９３】（Ｓ６２）領域Ｌ１のデータが読み出し済でないなら、メモリ３の作業域に、キーデータを展開する処理を行う。即ち、ＣＰＵ２は、パスワードＰＷｉを得る。そして、領域Ｌｉを読み出し、読みだしたデータをパスワードＰＷｉで復号化する。これにより、パスワードＰＷ１を得る

【００９４】（Ｓ６３）次に、ＣＰＵ２は、光ディスク１の領域Ｌ１のデータＰＳ’〔１〕～ＰＳ’〔ｎ〕を読みだす。ＣＰＵ２は、領域Ｌ１のデータＰＳ’〔１〕～ＰＳ’〔ｎ〕を、パスワードＰＷ１で復号化する。これにより、キーデータＰＳ〔１〕～ＰＳ〔ｎ〕が得られる。このキーデータＰＳ〔　〕（ＰＳ〔１〕～ＰＳ〔ｎ〕）を、メモリ３の作業域に格納する

【００９５】（Ｓ６４）ＣＰＵ２は、要求されたセクタ番号Ｓ０から４つの値Ｒ０、Ｒ１、Ｒ２、Ｒ３を得る。ここでは、論理セクタ番号Ｓ０を３２ビットのビット列と見なし、８ビットづつを１つの値Ｒ０、Ｒ１、Ｒ２、Ｒ３に割める。そして、Ｒ０～Ｒ３をインデックスとして、メモリ３の作業域のＰＳ〔　〕から乱数値（キーデータ）を取り出す。取り出した４つの値を基に、８バイトの乱数（キーデータ）Ｒを発生する

【００９６】ここでは、図９に示すように、Ｒ０に対応するキーデータＰＳ〔Ｒ０〕を取り出し、（Ｒ１＋２５６）に対応するキーデータＰＳ〔Ｒ１＋２５６〕を取り出す　Ｒ２に対応するキーデータＰＳ〔Ｒ２＋２５６〕を取り出し、Ｒ３に対応するキーデータＰＳ〔Ｒ３〕を取り出す

【００９７】そして、上述した演算式により、キーデータＲを演算する。

【００９８】（Ｓ６５）そして、ＣＰＵ２は、書き込むべきデータを、このキーデータＲで暗号化する。暗号化の方法としては、周知のＤＥＳ等を用いることができる。ＣＰＵ２は、この暗号化されたデータを、光ディスク１の論理ブロックアドレスＬＢＡ（＝Ｓ１）の位置に書き込む。

【００９９】このようにして、複数のユーザーパスワードを使用することができる。

【０１００】図１３は、本発明の第４の実施の形態のパスワード変更処理フロー図（その１）、図１４は、本発明の第４の実施の形態のパスワード変更処理フロー図（その２）である。

【０１０１】図１１の構成において、ユーザーパスワードＰＷ１を変更する処理について、図１３により、説明する。

【０１０２】（Ｓ７０）ＣＰＵ２は、旧パスワードＰＷ１と新パスワードＰＷ１’を得る

【０１０３】（Ｓ７１）ＣＰＵ２は、光ディスク１の領域Ｌ１と領域Ｃ１を読みだす

【０１０４】（Ｓ７２）ＣＰＵ２は、領域Ｌ１の暗号化されたキーデータを、パスワードＰＷ１で復号化して、キーデータＰＳ〔　〕を得る。そして、ＣＰＵ２は、領域Ｃ１のデータをパスワードＰＷ１で復号化する。更に、復号化された検証用文字列から、パスワードＰＷ１の正当性を判定する。パスワードが正しくなければ、エラーとする

【０１０５】（Ｓ７３）ＣＰＵ２は、キーデータＰＳ〔　〕を、新パスワードＰＷ１’で暗号化して、光ディスク１の領域Ｌ１に書き込む。

【０１０６】（Ｓ７４）次に、ＣＰＵ２は、新パスワードＰＷ１’に対する検証用文字列ＤＣ１’を作成する。そして、ＣＰＵ２は、検証用文字列ＤＣ１’を新パスワードＰＷ１’で暗号化して、書き込み値Ｃ１’を得る。更に、ＣＰＵ２は、書き込み値Ｃ１’を光ディスク１の領域Ｃ１に書き込む。

【０１０７】このようにして、旧パスワードの正当性を確認して、新パスワードに変更することができる。しかも、データの再暗号化を必要としないで、パスワードの変更ができる。この方法は、ユーザーパスワードが１つの場合に有効な方法である。

【０１０８】複数のユーザーパスワードを設定した場合には、図１３の処理を実行して、新パスワードに変更した場合に、ユーザーパスワードＰＷ２～ＰＷｎによるデータアクセスができなくなる。複数のユーザーパスワードを設定した場合にこれが不都合であるなら、パスワードＰＷ１をユーザーパスワードとして使用せずに、ユーザーパスワードＰＷｉ（ｉ＞１）のみを、使用者のパスワードとして使用すれば良い。

【０１０９】このユーザーパスワードＰＷｉ（ｉ＞１）を変更する処理を、図１４により説明する。

【０１１０】（Ｓ８０）ＣＰＵ２は、旧パスワードＰＷｉと新パスワードＰＷｉ’を得る。

【０１１１】（Ｓ８１）ＣＰＵ２は、光ディスク１の領域Ｌｉと領域Ｃｉを読みだす。

【０１１２】（Ｓ８２）ＣＰＵ２は、領域Ｌｉの暗号化されたデータを、パスワードＰＷｉで復号化して、パスワードＰＷ１を得る。そして、ＣＰＵ２は、領域ＣｉのデータをパスワードパスワードＰＷｉで復号化する。更に、復号化された検証用文字列から、パスワードＰＷｉの正当性を判定する。パスワードが正しくなければ、エラーとする。

【０１１３】（Ｓ８３）ＣＰＵ２は、パスワードＰＷ１を、新パスワードＰＷｉ’で暗号化して、光ディスク１の領域Ｌｉに書き込む。

【０１１４】（Ｓ８４）次に、ＣＰＵ２は、新パスワードＰＷｉ’に対する検証用文字列ＤＣｉ’を作成する。そして、ＣＰＵ２は、検証用文字列ＤＣｉ’を新パスワードＰＷｉ’で暗号化して、書き込み値Ｃｉ’を得る。更に、ＣＰＵ２は、書き込み値Ｃｉ’を光ディスク１の領域Ｃｉに書き込む。

【０１１５】このようにして、旧パスワードＰＷｉの正当性を確認して、パスワードＰＷｉを変更できる。この例も、データの再暗号化を必要としないで、パスワードの変更が可能である。

【０１１６】上述の実施の態様の他に、本発明は、次のような変形が可能である。

【０１１７】（１）記憶媒体を、光磁気ディスクで説明したが、光ディスク、磁気ディスク、ＩＣカード等他の記憶媒体に適用できる。

【０１１８】（２）乱数Ｒを求める演算式は、他の形式のものも利用できる。

【０１１９】以上、本発明の実施の形態により説明したが、本発明の主旨の範囲内で種々の変形が可能であり、これらを本発明の範囲から排除するものではない。

【０１２０】

【発明の効果】以上説明したように、本発明によれば、次の効果を奏する。

【０１２１】（１）パスワードをそのまま暗号化キーとして用いるのではなく、パスワードとは、別に生成したキーデータを用いて、データを暗号化する。暗号文を解析しても、暗号化されたキーデータが解読されるだけである。このため、パスワードやキーデータを解析しにくい。これにより、暗号文の解析によるパスワードの解読を防止できる。

【０１２２】（２）又、パスワードとは、別に生成したキーデータを用いて、暗号化するため、１つのパスワードに対し、キーデータを変えることにより、セクタ等の記憶単位に異なるキーを付与できる。このため、論理セクタ毎に異なるキーを用いて、暗号化でき、データの機密性を高めることができる。

【０１２３】（３）更に、パスワードとは、別に生成したキーデータを用いて、暗号化するため、パスワードを変えても、データの再暗号化が不要となる。このため、数百メガバイトの大容量記憶媒体でも、容易にパスワードの変更を実現できる。

【図面の簡単な説明】

【図１】本発明の一実施の形態のブロック図である。

【図２】本発明の第１の実施の形態の論理フォーマット時の処理フロー図である。

【図３】本発明の第１の実施の形態の書き込み処理フロー図である。

【図４】本発明の第１の実施の形態の記憶領域の説明図である。

【図５】本発明の第１の実施の形態のキーデータの説明図である。

【図６】本発明の第１の実施の形態の読み出し処理フロー図である。

【図７】本発明の第２の実施の形態の書き込み処理フロー図である

【図８】本発明の第３の実施の形態の書き込み処理フロー図である。

【図９】本発明の第３の実施の形態のキーデータの説明図である

【図１０】本発明の第３の実施の形態の読み出し処理フロー図である

【図１１】本発明の第４の実施の形態の説明図である

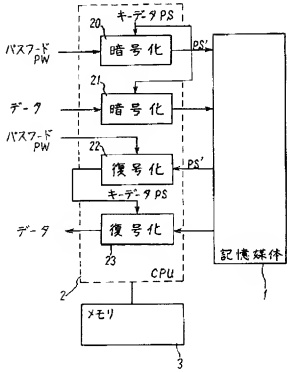
【図１２】本発明の第４の実施の形態の書き込み処理フロー図である

【図１３】本発明の第４の実施の形態のパスワード変更

処理フロー図（その1）である。
【図14】本発明の第4の実施の形態のパスワード変更処理フロー図（その2）である。
【図15】従来技術の説明図である。
【符号の説明】
1　光ディスク（記憶媒体）
＊2　制御回路（CPU）
3　メモリ
20　第1の暗号化部
21　第2の暗号化部
22　第1の復号化部
23　第2の復号化部

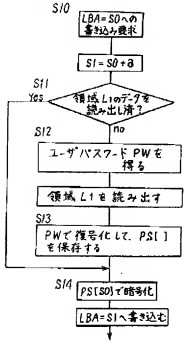
【図1】

ブロック図



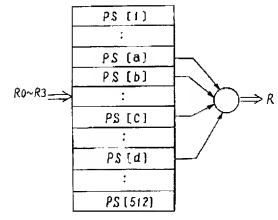
【図3】

書き込み処理フロー図



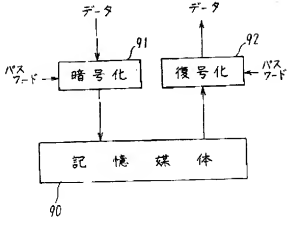
【図9】

キーデータの説明図



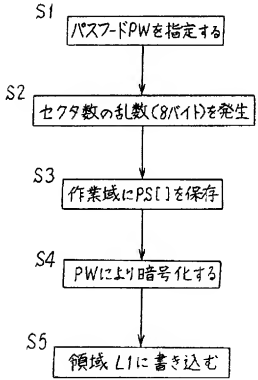
【図15】

従来技術の説明図



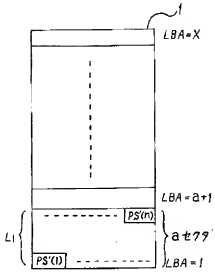
【図2】

論理フォーマット時の処理フロー図



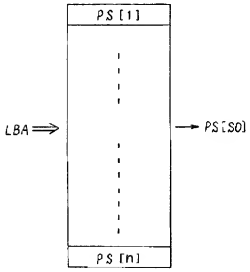
【図4】

記憶領域の説明図



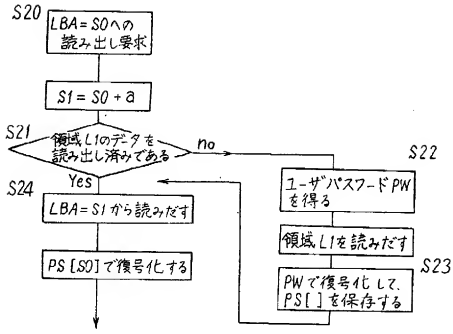
【図5】

キーデータの説明図



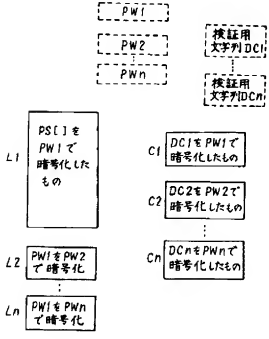
【図6】

読み出し処理フロー図



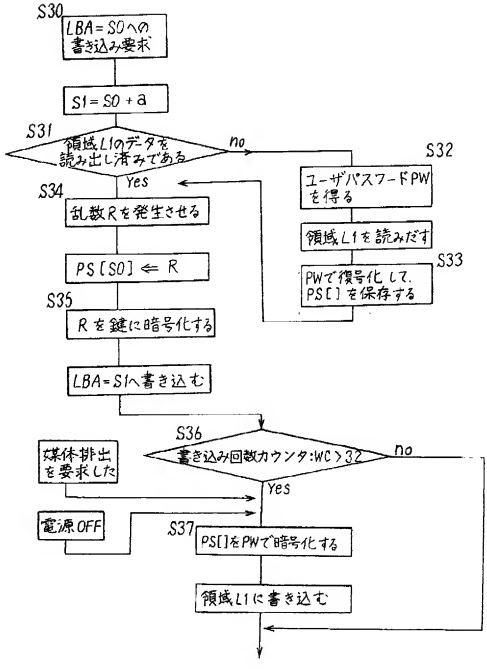
【図11】

第4の実施の形態の説明図



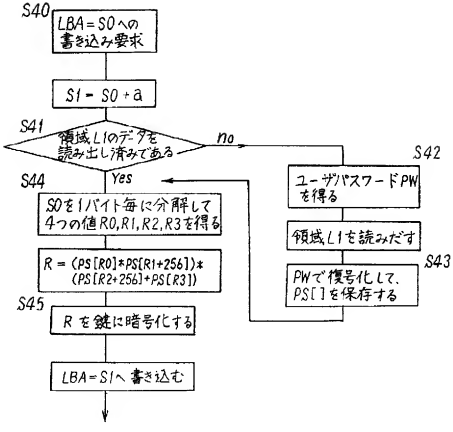
【図7】

書き込み処理フロー図



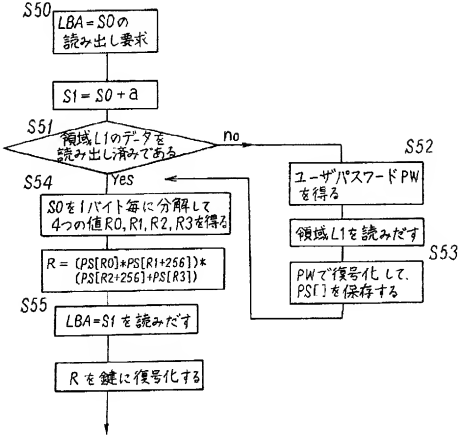
【図8】

書き込み処理フロー図



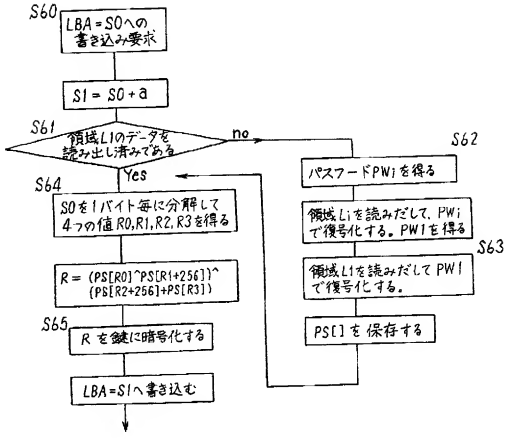
【図10】

読み出し処理フロー図



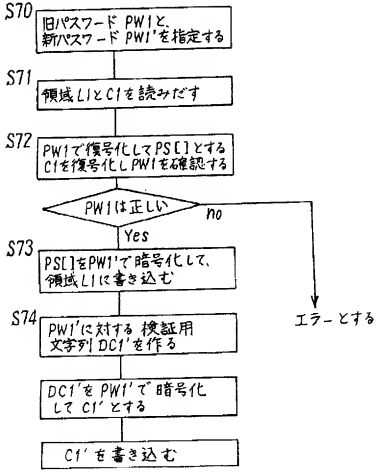
【図１２】

書き込み処理フロー図



【図１３】

パスワード変更処理フロー図（その１）



【図１４】

パスワード変更処理フロー図（その２）